New Families of Binary Sequences with Optimal Three-Level Autocorrelation

Cunsheng Ding, *Member, IEEE*, Tor Helleseth, *Fellow, IEEE*, and Halvard Martinsen

***Abstract*—In this correspondence we give several new families of binary sequences of period N with optimal three-level autocorrelation, where $N \equiv 2 (\mod 4)$. These sequences are either balanced or almost balanced. Our construction is based on cyclotomy.**

***Index Terms*—Almost difference sets, optimal autocorrelation, sequences.**

I. Introduction

Given a binary sequence $\{s(t)\}$ of period N, the autocorrelation of the sequence at shift w is defined by

$$C_s(w) = \sum_{t=0}^{N-1} (-1)^{s(t+w)-s(t)}.$$

An important problem in sequence design is to find sequences with optimal autocorrelation, i.e., where $C_s(w) = -1$ if $N \equiv 1(\mod 2)$, $C_s(w) = -2$ and 2 if $N \equiv 2(\mod 4)$, and $C_s(w) \in \{0, -4\}$ if $N \equiv 0(\mod 4)$ for any $w \not\equiv 0(\mod N)$. For many applications, such as code-division multiple access (CDMA) communications and stream ciphering [3], [11], [13], [20], we are interested in constructing sequences of period N with optimal autocorrelation and where k, the number of 1s in a periodic segment, is very close to $N/2$.

Sequences with optimal autocorrelation of odd period have been studied for several decades and this has resulted in numerous constructions. These are of considerable interest also because of their close connections to difference sets.

For even N there are only two constructions of binary sequences with optimal autocorrelation. One is by Lempel, Cohn, and Eastman [16], which gives balanced binary sequences of period $p^m - 1$ for odd prime p. Recently, No, Chung, Song, Yang, Lee, and Helleseth [17] gave a new construction of almost balanced binary sequences of period $p^m - 1$, p odd prime, with optimal autocorrelation. They also found a new description and a simpler proof of the optimal autocorrelation sequences by Lempel, Cohn, and Eastman [16].

In this correspondence, we will give several new families of binary sequences of period $N = 2p$ with optimal autocorrelation, where $p \equiv 5(\mod 8)$ is prime and has a quadratic partition of form either $p = x^2 + 4$ or $p = 1 + 4y^2$. It is the first construction of families with optimal autocorrelation where $N \neq p^m - 1$, for p prime. The sequences will be either balanced or almost balanced, that is, two more zeros than ones in each period. See Table I for all the lengths $N \leq 3000$ our construction applies for. Note that every prime $p \equiv 1(\mod 4)$ has a quadratic partition $p = x^2 + 4y^2$, and that every quadratic form $x^2 + by^2$ represents infinitely many primes [2], where $b \neq 0$. Thus the constructions of this correspondence give indeed several classes of infinitely many binary sequences with optimal autocorrelation.

TABLE I
Sequences of Length N With Optimal Autocorrelation Covered by Theorems in This Paper (Length N Marked With * Satisfies $N \neq p^m - 1$, p Prime, $m \geq 1$)

Period $N = 2p$	Prime p	Optimal autocorrelation by theorem
10	5	Theorem 1, 2, 3, 4
26	13	Theorem 1, 3
58	29	Theorem 1, 3
74*	37	Theorem 2, 4
106	53	Theorem 1, 3
202*	101	Theorem 2, 4
346	173	Theorem 1, 3
394*	197	Theorem 2, 4
458*	229	Theorem 1, 3
586	293	Theorem 1, 3
1354*	677	Theorem 2, 4
1466*	733	Theorem 1, 3
2186	1093	Theorem 1, 3
2458	1229	Theorem 1, 3
2746*	1373	Theorem 1, 3

Our construction is based on cyclotomy. Essentially, we will find a subset C of $\boldsymbol{Z}_N$ and define the *characteristic sequence* $\{s(t)\}$ of C as

$$s(t) = \begin{cases} 1, & \text{if } t \bmod N \in C \\ 0, & \text{otherwise.} \end{cases}$$

On the other hand, we will say that C is the *characteristic set* or *support* of $\{s(t)\}$. The autocorrelation property is determined by the difference function defined as

$$d_C(w) = |(w + C) \cap C|$$

where $w + C$ denotes the set $\{w + c\colon c \in C\}$ and "+" denotes addition modulo N.

Lemma 1: [3, p. 143]: Let $\{s(t)\}$ be a binary sequence of period N. Then

$$C_s(w) = N - 4(k - d_C(w))$$

where $k = |C|$.

In the case $N \equiv 1(\mod 2)$, sequences with optimal autocorrelation are heavily related to difference sets, see for example, [1], [12], [10], [14], [15], [18], and [19]. For even N, the sequences with optimal autocorrelation are related to *almost difference sets*. Let $N > 1$, $|C| = k$, and $d_C(w)$ be defined as above. We call C an (N, k, λ, t) almost difference set of $\boldsymbol{Z}_N$ if $d_C(w)$ takes on the value λ altogether t times and the value $\lambda + 1$ altogether $N - 1 - t$ times when w ranges over all the nonzero elements of $\boldsymbol{Z}_N$. The almost difference sets introduced here are a generalization of the almost difference sets introduced by Ding [6], [7] (see also [3, p. 140]) and the almost difference sets introduced by Davis [4]. It is nice that this generalization unifies the two kinds of existing almost difference sets.

For (N, k, λ, t) almost difference sets of $\boldsymbol{Z}_N$ we have the following basic relation:

$$k(k-1) = t\lambda + (N - 1 - t)(\lambda + 1). \tag{1}$$

Manuscript received October 10, 1999; revised June 30, 2000.

C. Ding is with the Department of Computer Science, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (e-mail: cding@cs.ust.hk).

T. Helleseth and H. Martinsen are with the Department of Informatics, University of Bergen, HIB, N-5020 Bergen, Norway (e-mail: torh@ii.uib.no; halvard@ii.uib.no).

Communicated by S. W. Golomb, Associate Editor for Sequences.

Publisher Item Identifier S 0018-9448(01)00584-3.

By Lemma 1, a binary sequence $\{s(t)\}$ of period $N \equiv 2 (\bmod 4)$ has optimal autocorrelation values 2 and -2 if and only if its support $\{i \in \boldsymbol{Z}_N \colon s_i = 1\}$ is an

$$(N, k, k-(N+2)/4, (N-1)(k-(N-2)/4)-k(k-1))$$

almost difference set of $\boldsymbol{Z}_N$. Hence the binary sequences obtained in this correspondence give also several classes of new almost difference sets of $\boldsymbol{Z}_N$ with parameters $(N, N/2-1, (N-6)/4, 3(N-2)/4)$, $(N, N/2+1, (N+2)/4, 3(N-2)/4)$, and $(N, N/2, (N-2)/4, (3N-2)/4)$, respectively.

II. The Idea of our Construction

We will in this section present a general construction of a characteristic set C for a sequence $\{s(t)\}$ of period $N = 2p$, where p is an odd prime. The difference function will be evaluated, such that it will be easy to find the autocorrelation values for a given construction.

Since, $N \equiv 2 (\bmod 4)$, finding sequences with optimal autocorrelation will be equivalent to constructing almost difference sets, as made clear at the end of the previous section.

By the Chinese Remainder Theorem, $\boldsymbol{Z}_N \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_p$ under the isomorphism $\phi \colon w \mapsto (w \bmod 2, w \bmod p)$, see [9]. Construction of almost difference sets over $\boldsymbol{Z}_N$ is, therefore, equivalent to construction over $\boldsymbol{Z}_2 \times \boldsymbol{Z}_p$.

Let $C = \{0\} \times C_0 \cup \{1\} \times C_1$, where $C_i \subseteq \boldsymbol{Z}_p$, $0 \le i \le 1$. Define $w = (w_1, w_2) \in \boldsymbol{Z}_2 \times \boldsymbol{Z}_p$. Then we may evaluate the difference function as follows:

$$\begin{aligned} d_C(w_1, w_2) &= |C \cap (C + (w_1, w_2))| \\ &= |\{0\} \cap \{w_1\}||C_0 \cap (C_0 + w_2)| \\ &\quad + |\{0\} \cap \{1 + w_1\}||C_0 \cap (C_1 + w_2)| \\ &\quad + |\{1\} \cap \{w_1\}||C_1 \cap (C_0 + w_2)| \\ &\quad + |\{1\} \cap \{1 + w_1\}||C_1 \cap (C_1 + w_2)| \\ &= \begin{cases} |C_0 \cap (C_0 + w_2)| + |C_1 \cap (C_1 + w_2)|, & w_1 = 0 \\ |C_0 \cap (C_1 + w_2)| + |C_1 \cap (C_0 + w_2)|, & w_1 = 1 \end{cases} \\ &= \begin{cases} |C_0| + |C_1|, & \text{if } w_1 = 0,\ w_2 = 0, \\ |C_0 \cap (C_0 + w_2)| + |C_1 \cap (C_1 + w_2)|, & \\ & \text{if } w_1 = 0,\ w_2 \neq 0 \\ |C_0 \cap (C_1 + w_2)| + |C_1 \cap (C_0 + w_2)|, & \\ & \text{if } w_1 = 1,\ w_2 \neq 0 \\ 2|C_0 \cap C_1|, & \text{if } w_1 = 1,\ w_2 = 0 \end{cases} \end{aligned} \tag{2}$$

where $k = |C| = |C_0| + |C_1|$. If C is an almost difference set and a characteristic set for an optimal autocorrelation sequence $\{s(t)\}$ of length $N = 2p$, then by Lemma 1

$$|C_0 \cap C_1| = \frac{2k - p \pm 1}{4}.$$

Thus if $k = p$, then $|C_0 \cap C_1| = \frac{p \pm 1}{4}$. If $k = p-1$, then $|C_0 \cap C_1| = \frac{p-1}{4}$ or $\frac{p-3}{4}$. This gives us some hint about how we should choose our C_i. In the following two sections, we shall use cyclotomic classes to form our C_i and then look for conditions to ensure that our C is an almost difference set. Such an almost difference set will give a binary sequence with optimal autocorrelation.

III. Almost Balanced Sequences with Optimal Three-Level Autocorrelation

Let GF(q) be a finite field, and let d divide $q-1$. For a primitive element α of GF(q), define $D_0^{(d,q)} = (\alpha^d)$, the multiplicative group generated by α^d, and

$$D_i^{(d,q)} = \alpha^i D_0^{(d,q)}, \qquad \text{for } i = 1, 2, \ldots, d-1.$$

These $D_i^{(d,q)}$ are called *cyclotomic classes* of order d. The *cyclotomic numbers* of order d with respect to GF(q) are defined as

$$(i, j) = |(D_i^{(d,q)} + 1) \cap D_j^{(d,q)}|.$$

Clearly, there are at most d^2 different cyclotomic numbers of order d. Let $p = 4f + 1$ be a prime. In the remainder of this section, we consider cyclotomic classes $D_i^{(4,p)}$ with respect to p and cyclotomic numbers of order 4. For simplicity, let D_i denote $D_i^{(4,p)}$. Let $p = x^2 + 4y^2$, where $x, y \in \boldsymbol{Z}$ and $x \equiv 1 \bmod 4$. Here y is two-valued, depending on the choice of the primitive root α employed to define the cyclotomic classes [5], [3]. There are at most five distinct cyclotomic numbers when f is odd, which are

$$\begin{aligned} (0,0) &= (2,2) = (2,0) = (p - 7 + 2x)/16 \\ (0,1) &= (1,3) = (3,2) = (p + 1 + 2x - 8y)/16 \\ (1,2) &= (0,3) = (3,1) = (p + 1 + 2x + 8y)/16 \\ (0,2) &= (p + 1 - 6x)/16 \\ \text{the rest} &= (p - 3 - 2x)/16. \end{aligned}$$

There is also a theory for cyclotomic numbers when f is even. We do not explicitly use these numbers, and they are therefore omitted.

Now we are ready to construct several classes of binary sequences of period $N = 2p$ with optimal autocorrelation. Define

$$C_0 = D_i \bigcup D_j, \; C_1 = D_l \bigcup D_j$$

where i, j, and l are pairwise distinct integers between 0 and 3.

It is then clear that

$$|C_0| = |C_1| = \frac{p-1}{2} \quad \text{and} \quad |C_0 \cap C_1| = \frac{p-1}{4}.$$

We now define

$$C = \{0\} \times C_0 \cup \{1\} \times C_1.$$

Then by (2)

$$d_C(w_1, w_2) = \begin{cases} |C_0| + |C_1|, & \text{if } w_1 = 0,\ w_2 = 0 \\ |C_0 \cap (C_0 + w_2)| + |C_1 \cap (C_1 + w_2)|, & \\ & \text{if } w_1 = 0,\ w_2 \neq 0 \\ |C_0 \cap (C_1 + w_2)| + |C_1 \cap (C_0 + w_2)|, & \\ & \text{if } w_1 = 1,\ w_2 \neq 0 \\ 2|C_0 \cap C_1|, & \text{if } w_1 = 1,\ w_2 = 0. \end{cases}$$

Notice that

$$|C_i \cap (C_j + w_2)| = |w_2^{-1} C_i \cap (w_2^{-1} C_j + 1)|.$$

If $w_2^{-1} \in D_h$, then the above equation equals a sum of four cyclotomic numbers. Using this relation, straightforward calculations give

$$d_C(w_1,\, w_2) = \begin{cases} p-1, & \text{if } w_1 = 0,\ w_2 = 0, \\ \\ (i+h,\, i+h) + 2(j+h,\, j+h) \\ +(l+h,\, l+h) + (j+h,\, i+h) \\ +(i+h,\, j+h) + (j+h,\, l+h) \\ +(l+h,\, j+h), & \text{if } w_1 = 0,\ w_2^{-1} \in D_h \\ \\ (j+h,\, i+h) + (l+h,\, i+h) \\ +2(j+h,\, j+h) + (l+h,\, j+h) \\ +(i+h,\, j+h) + (i+h,\, l+h) \\ +(j+h,\, l+h), & \text{if } w_1 = 1,\ w_2^{-1} \in D_h \\ \\ \frac{p-1}{2}, & \text{if } w_1 = 1,\ w_2 = 0. \end{cases} \tag{3}$$

We will include some results on the different choices of $(i,\, j,\, l)$ corresponding to different symmetry relations on sequences. The triple $(i,\, j,\, l)$ will be called the defining set for the sequence $\{s(t)\}$ given by

$$s(t) = \begin{cases} 1, & \text{if } t \in D = \phi^{-1}(C) \\ 0, & \text{otherwise.} \end{cases}$$

Notice that D in the above equation is the characteristic set for $\{s(t)\}$. The definition of D as $\phi^{-1}(C)$ will be used in the remainder of the correspondence.

Lemma 2: If $(i,\, j,\, l)$ is a defining set for $\{s(t)\}$, then $(l,\, j,\, i)$ is a defining set for $\{s(t + N/2)\}$.

Proof: Observe that C is given by

$$C = (\{0\} \times (D_i \cup D_j)) \cup (\{1\} \times (D_l \cup D_j))$$

and that shifting the corresponding sequence by $N/2$ is the same as adding $(1,\, 0)$ to the above expression. As a result, we get

$$C = (\{1\} \times (D_i \cup D_j)) \cup (\{0\} \times (D_l \cup D_j))$$

which proves the lemma. □

Lemma 3: If (i, j, l) is a defining set for $\{s(t)\}$, then $(i+2, j+2, l+2)$ is a defining set for $\{s(N-t)\}$.

Proof: The characteristic sequence $\{s(t)\}$ of D with defining set $(i,\, j,\, l)$ has $s(t) = 1$ if and only if

$$\phi(t) \in (\{0\} \times (D_i \cup D_j)) \cup (\{1\} \times (D_l \cup D_j))$$

and $s(N - t) = 1$ if and only if

$$\phi(t) \in (\{-0\} \times (-D_i \cup -D_j)) \cup (\{-1\} \times (-D_l \cup -D_j))$$

where ϕ is the mapping in the Chinese Remainder Theorem given in the beginning of Section II. Notice that $-1 = \alpha^{\frac{p-1}{2}} = \alpha^{2f} \in D_2$, such that the above equation reduces to

$$\phi(t) \in (\{0\} \times (D_{i+2} \cup D_{j+2})) \cup (\{1\} \times (D_{l+2} \cup D_{j+2}))$$

which proves the lemma. □

Recall from Lemma 1 that the autocorrelation at shift w was given as $\mathrm{C_s(w)} = N - 4(k - d_C(w))$. We are interested in the case where $C_s(w) = -2p + 4 + 4d_C(w) \in \{-2,\, +2\}$, when $w \neq 0$ and $k = p - 1$. The autocorrelation values are only dependent on the difference function. The next result gives us the evaluation of this function for a certain defining set $(i,\, j,\, l)$.

Lemma 4: For $(i,\, j,\, l) = (0,\, 1,\, 3)$, we have

$$d_C(w_1,\, w_2) = \begin{cases} \frac{p-2-y}{2}, & w_1 = 0,\ w_2^{-1} \in D_0 \cup D_2 \\ \frac{p-4+y}{2}, & w_1 = 0,\ w_2^{-1} \in D_1 \cup D_3 \\ \frac{p-1}{2}, & w_1 = 1,\ w_2^{-1} \in D_0 \cup D_2 \\ \frac{p-3}{2}, & w_1 = 1,\ w_2^{-1} \in D_1 \cup D_3 \\ \frac{p-1}{2}, & w_1 = 1,\ w_2 = 0. \end{cases}$$

Proof: Straightforward calculations using the cyclotomic numbers and (3) proves the lemma. □

In the same manner, we may calculate $d_C(w_1,\, w_2)$ for possible defining sets $(i,\, j,\, l)$. We will use several distinct defining sets in the following results. Since the evaluation of $d_C(w_1,\, w_2)$ is straightforward, but tedious, we omit the results which are similar to Lemma 4.

Theorem 1: Let $p = 4f + 1 = x^2 + 4y^2$, where $y = 1$ and f is odd. The length $N = 2p$ characteristic sequence $\{s(t)\}$ of D has optimal autocorrelation if $(i,\, j,\, l) = (0,\, 1,\, 3)$ or $(0,\, 2,\, 1)$.

Proof: The difference function can be calculated for all choices of $(i,\, j,\, l)$ as in Lemma 4. For $(i,\, j,\, l) = (0,\, 1,\, 3)$ and $(0,\, 2,\, 1)$ when $y = 1$ the value set of $d_C(w_1,\, w_2)$ is

$$d_C(w_1,\, w_2) = \frac{p-1}{2} \text{ or } \frac{p-3}{2}$$

whenever $(w_1,\, w_2) \neq (0,\, 0)$. From Lemma 1 we obtain

$$\begin{aligned} C_s(w_1,\, w_2) &= N - 4(k - d_C(w_1,\, w_2)) \\ &= 2p - 4(p - 1 - d_C(w_1,\, w_2)) \\ &= -2p + 4 + 4d_C(w_1,\, w_2) \in \{-2,\, +2\} \end{aligned}$$

when $(w_1,\, w_2) \neq (0,\, 0)$. □

Theorem 2: Let $p = 4f + 1 = x^2 + 4y^2$, where $x = 1$ and f is odd. The length $N = 2p$ characteristic sequence $\{s(t)\}$ of D has optimal autocorrelation if $(i,\, j,\, l) = (1,\, 0,\, 3)$ or $(0,\, 1,\, 2)$.

Proof: By (3) and cyclotomic numbers of order 4, we have

$$d_C(w_1,\, w_2) = \begin{cases} \frac{p-3}{2}, & w_1 = 0,\ w_2 \neq 0 \\ \frac{p-2-x}{2}, & w_1 = 1,\ w_2^{-1} \in D_0 \cup D_2 \\ \frac{p-2+x}{2}, & w_1 = 1,\ w_2^{-1} \in D_1 \cup D_3 \\ \frac{p-1}{2}, & w_1 = 1,\ w_2 = 0 \end{cases}$$

for the defining set $(i,\, j,\, l) = (0,\, 1,\, 2)$. For $(i,\, j,\, l) = (1,\, 0,\, 3)$ the same values will occur. As in Theorem 1

$$d_C(w_1,\, w_2) = \frac{p-1}{2} \text{ or } \frac{p-3}{2}$$

whenever $(w_1,\, w_2) \neq (0,\, 0)$. The results now follow from Lemma 1. □

Example 1: To illustrate the sequences described in Theorem 2, we consider the following example. Take $p = 5 = 1 + 4 \times 1^2 = 5$, and define $N = 2p = 10$. We use the primitive root 2 modulo 5 to define the cyclotomic classes. Then $D_0 = \{1\}$, $D_1 = \{2\}$, $D_2 = \{4\}$, and $D_3 = \{3\}$. We take $(i,\, j,\, l) = (1,\, 2,\, 3)$. Then $C_0 = \{2,\, 4\}$ and $C_1 = \{3,\, 4\}$. Hence $\phi^{-1}(C) = \{2,\, 3,\, 4,\, 9\}$. The corresponding characteristic sequence is

$$\{s(t)\} = \underbrace{0011100001}\ldots$$

which has optimal autocorrelation.

Remarks:

1) In each periodic segment of all the sequences of period N in this section, the number of 1s and 0s is $N/2 - 1$ and $N/2 + 1$, respectively. We say that such a sequence is almost balanced in the case $N \equiv 2 \pmod 4$.
2) The autocorrelation function of each binary sequence given in this section takes on -2 altogether $3(N-2)/4$ times and 2 altogether $(N+2)/4$ times. This conclusion follows from the proofs of all the theorems in this section, and also the statement about almost difference sets at the end of Section I.
3) The complement sequence of each sequence given in this section also has optimal autocorrelation.
4) For each triple (i, j, l) we may calculate the difference function and thereby the autocorrelation of the corresponding sequence.

IV. Balanced Sequences with Optimal Three-Level Autocorrelation

The sequences with optimal three-level autocorrelation constructed in the previous section are almost balanced. In this section, we modify the construction and give several classes of balanced binary sequences with optimal three-level autocorrelation.

In this section, we define the sets C in a slightly different way. Now we complement the bit in position 0 or p of the sequences given in the previous section. As in the previous section, let

$$C_0 = D_i \cup D_j, \quad C_1 = D_l \cup D_j$$

where i, j, and l are pairwise distinct integers between 0 and 3. To complement the bit in position 0, define

$$C^0 = (\{0\} \times C_0) \cup (\{1\} \times C_1) \cup \{(0, 0)\}$$

and to complement the bit in position p, define

$$C^p = (\{0\} \times C_0) \cup (\{1\} \times C_1) \cup \{(1, 0)\}$$

and the corresponding characteristic set for the sequence $\{s(t)\}$ as

$$D^0 = \phi^{-1}(C^0)$$

and

$$D^p = \phi^{-1}(C^p).$$

As we did for (3), we must calculate the difference function for C^0 and C^p. For C^p

$$\begin{aligned} d_{C^p}(w_1, w_2) &= |C^p \cap (C^p + (w_1, w_2))| \\ &= |C \cap (C + (w_1, w_2))| + |(1, 0) \cap (C + (w_1, w_2))| \\ &\quad + |(1, 0) \cap (1 + w_1, w_2)| + |C \cap (1 + w_1, w_2)|. \end{aligned}$$

Clearly, if $(w_1, w_2) \neq (0, 0)$, then

$$d_{C^p}(w_1, w_2) = d_C(w_1, w_2) + \Delta(w_1, w_2)$$

where $d_C(w_1, w_2)$ is as stated in (3) and

$$\begin{aligned} \Delta(w_1, w_2) &= |(1, 0) \cap (w_1, C_0 + w_2)| \\ &\quad + |(1, 0) \cap (1 + w_1, C_1 + w_2)| \\ &\quad + |(1 + w_1, w_2) \cap (0, C_0)| \\ &\quad + |(1 + w_1, w_2) \cap (1, C_1)| \\ &= \begin{cases} |\{w_2\} \cap C_1| + |\{0\} \cap (C_1 + w_2)|, & \\ & \text{if } w_1 = 0,\ w_2 \neq 0 \\ |\{w_2\} \cap C_0| + |\{0\} \cap (C_0 + w_2)|, & \\ & \text{if } w_1 = 1,\ w_2 \neq 0, \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} |C_1 \cap \{w_2, -w_2\}|, & w_1 = 0,\ w_2 \neq 0 \\ |C_0 \cap \{w_2, -w_2\}|, & w_1 = 1,\ w_2 \neq 0 \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Similarly, for C^0 we get for $(w_1, w_2) \neq (0, 0)$

$$\begin{aligned} d_{C^0}(w_1, w_2) &= d_C(w_1, w_2) \\ &\quad + \begin{cases} |C_0 \cap \{w_2, -w_2\}|, & w_1 = 0,\ w_2 \neq 0 \\ |C_1 \cap \{w_2, -w_2\}|, & w_1 = 1,\ w_2 \neq 0 \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{4}$$

The symmetry properties, similar to Lemma 2 and Lemma 3, are given by the two following results.

Lemma 5: Let D^0, defined by (i, j, l), be the characteristic set for $\{s(t)\}$, then the characteristic set for $\{s(t + N/2)\}$ is D^p, defined by (l, j, i).

Proof: Observe that C^0 is given by

$$C^0 = (\{0\} \times (D_i \cup D_j \cup \{0\})) \cup (\{1\} \times (D_l \cup D_j))$$

and that shifting the corresponding sequence by $N/2$ is the same as adding $(1, 0)$ to the above expression. As a result we get

$$C = (\{1\} \times (D_i \cup D_j \cup \{0\})) \cup (\{0\} \times (D_l \cup D_j))$$

which proves the lemma. □

Lemma 6: Let D^0 (or D^p) be the characteristic set, defined by (i, j, l) (resp., (i, j, l)), for $\{s(t)\}$, then $(i + 2, j + 2, l + 2)$ (resp., $(i + 2, j + 2, l + 2)$) is a defining set for $\{s(N - t)\}$.

Proof: The characteristic sequence $\{s(t)\}$ of C^0 with defining set (i, j, l) has $s(t) = 1$ if and only if

$$\phi(t) \in (\{0\} \times (D_i \cup D_j \cup \{0\})) \cup (\{1\} \times (D_l \cup D_j))$$

and $s(N - t) = 1$ if and only if

$$\phi(t) \in (\{0\} \times (-D_i \cup -D_j \cup \{0\})) \cup (\{1\} \times (-D_l \cup -D_j)).$$

Notice that $-1 = \alpha^{\frac{p-1}{2}} = \alpha^{2f} \in D_2$, such that the above equation reduces to

$$\phi(t) \in (\{0\} \times (D_{i+2} \cup D_{j+2} \cup \{0\})) \cup (\{1\} \times (D_{l+2} \cup D_{j+2})).$$

The result for D^p is proven in the same manner. □

Theorem 3: Let $p = 4f + 1 = x^2 + 4y^2$, where $y = 1$ and f is odd. Then the length $N = 2p$ characteristic sequence $\{s(t)\}$ of D^0 is balanced and has optimal autocorrelation if

$$(i, j, l) \in \{(0, 1, 3), (0, 2, 3), (1, 2, 0), (1, 3, 0)\}.$$

Proof: We have given $d_C(w_1, w_2)$ by Lemma 4 for $(i, j, l) = (0, 1, 3)$. By (4)

$$d_{C^0}(w_1, w_2) = \begin{cases} \frac{p-2-y}{2}, & w_1 = 0,\ w_2^{-1} \in D_0 \cup D_2, \\ & \pm w_2 \notin D_0 \cup D_1 \\ \frac{p-y}{2}, & w_1 = 0,\ w_2^{-1} \in D_0 \cup D_2, \\ & \pm w_2 \in D_0 \cup D_1 \\ \frac{p-4+y}{2}, & w_1 = 0,\ w_2^{-1} \in D_1 \cup D_3, \\ & \pm w_2 \notin D_0 \cup D_1 \\ \frac{p-2+y}{2}, & w_1 = 0,\ w_2^{-1} \in D_1 \cup D_3, \\ & \pm w_2 \in D_0 \cup D_1 \\ \frac{p-1}{2}, & w_1 = 1,\ w_2^{-1} \in D_0 \cup D_2, \\ & \pm w_2 \notin D_1 \cup D_3 \\ \frac{p+1}{2}, & w_1 = 1,\ w_2^{-1} \in D_0 \cup D_2, \\ & \pm w_2 \in D_1 \cup D_3 \\ \frac{p-3}{2}, & w_1 = 1,\ w_2^{-1} \in D_1 \cup D_3, \\ & \pm w_2 \notin D_1 \cup D_3 \\ \frac{p-1}{2}, & w_1 = 1,\ w_2^{-1} \in D_1 \cup D_3, \\ & \pm w_2 \in D_1 \cup D_3 \\ \frac{p-1}{2}, & w_1 = 1,\ w_2 = 0. \end{cases}$$

Observe that the value $\frac{p+1}{2}$ never will occur, since the condition

$$w_2^{-1} \in D_0 \cup D_2,\ \pm w_2 \in D_1 \cup D_3$$

is impossible for w_2 to satisfy. The other defining set is proved in a similar manner. The conclusion then follows from Lemma 1. □

Theorem 4: Let $p = 4f + 1 = x^2 + 4y^2$, where $x = 1$ and f is odd. Then the length $N = 2p$ characteristic sequence $\{s(t)\}$ of D^0 is balanced and has optimal autocorrelation if

$$(i,\ j,\ l) \in \{(0,\ 1,\ 2),\ (0,\ 3,\ 2),\ (1,\ 0,\ 3),\ (1,\ 2,\ 3)\}.$$

Proof: The conclusion follows by using the same approach as in Theorem 3. □

Example 2: To illustrate one of the sequences described in Theorem 4, we consider the following example. Take $p = 5 = 1 + 4 \times 1^2 = 5$, and define $N = 2p = 10$. We use the primitive root 2 modulo 5 to define the cyclotomic classes. Then $D_0 = \{1\}$, $D_1 = \{2\}$, $D_2 = \{4\}$, and $D_3 = \{3\}$. We take $(i,\ j,\ l) = (1,\ 2,\ 3)$. Then $C_0 = \{2,\ 4\}$ and $C_1 = \{3,\ 4\}$. Hence $D^0 = \phi^{-1}(C^0) = \{0,\ 2,\ 3,\ 4,\ 9\}$. The corresponding characteristic sequences of D^0 is

$$\{s(t)\} = \underbrace{1011100001}\ldots$$

which has optimal autocorrelation and is balanced.

Remarks:

1) In each periodic segment of all the sequences of period N in this section, the number of 1s and 0s are $N/2$. So they are balanced.
2) The autocorrelation function of each binary sequence given in this section takes on -2 altogether $(3N-2)/4$ times and 2 altogether $(N-2)/4$ times. This conclusion follows from the proofs of all the theorems in this section, and also from the statement about almost difference sets at the end of Section I.
3) The complement sequences of the sequences given in this section also have optimal autocorrelation.

V. Concluding Remarks

All the sequences with optimal autocorrelation described in this correspondence have period $2p$, where $p \equiv 5 \pmod 8$ is a prime. We have not been able to construct any family of such sequences with period $2p$ by using cyclotomic classes of order 4, where $p \equiv 1 \pmod 8$ and is a prime. It is important to note that the families of sequences constructed in this correspondence are different from those described in [16] and [17], as some integers $2p$ are not in the form $q^m - 1$, where q is an odd prime, see Table I.

One may wonder whether it is possible to construct binary sequences of period $N \equiv 2 \pmod 4$ with cyclotomic classes of order 8 by defining

$$C_0 = D_m^{(8,\,p)} \cup D_n^{(8,\,p)} \cup D_i^{(8,\,p)} \cup D_j^{(8,\,p)}$$
$$C_1 = D_u^{(8,\,p)} \cup D_v^{(8,\,p)} \cup D_i^{(8,\,p)} \cup D_j^{(8,\,p)}$$
$$C = \{0\} \times C_0 \cup \{1\} \cup C_1$$

where $D_h^{(8,\,p)}$ are cyclotomic classes of order 8 and $p \equiv 1 \pmod 8$. We have tested many possible values for $m,\ n,\ i,\ j,\ u$, and v, but have not found any sequence with optimal autocorrelation.

As far as the construction of binary sequences with optimal autocorrelation is concerned, there are many open problems. Below are some of them.

1) Construct families of sequences of period $N \equiv 3 \pmod 4$ with optimal autocorrelation values -1 and 3, where $k = (N-3)/2$. This problem is equivalent to finding
$$(N,\ (N-3)/2,\ (N-7)/4,\ N-3)$$
almost difference sets of $\boldsymbol{Z}_N$.
2) In addition to the binary sequences of period $N \equiv 1 \pmod 4$ constructed in [7], [3], [8], where $k = (N-1)/2$, construct other families of sequences of such a period with optimal autocorrelation. This is equivalent to finding
$$(N,\ (N-1)/2,\ (N-5)/4,\ (N-1)/2)$$
almost difference sets of $\boldsymbol{Z}_N$.
3) Construct families of sequences of period $N \equiv 1 \pmod 4$ with optimal autocorrelation values -1 and 3, where $k = (N-3)/2$. This problem is equivalent to finding
$$(N,\ (N-3)/2,\ (N-9)/4,\ (N-5)/2$$
almost difference sets of $\boldsymbol{Z}_N$.
4) In addition to the binary sequences of period $N \equiv 2 \pmod 4$ constructed in [16], [17], and this correspondence, where $k = N/2 - 1$ and $N/2$, construct other families of sequences of such a period with optimal autocorrelation. This is equivalent to finding
$$(N,\ N/2-1,\ (N-6)/4,\ 3(N-2)/4)$$
and
$$(N,\ N/2,\ (N-2)/4,\ (3N-2)/4)$$
almost difference sets of $\boldsymbol{Z}_N$.
5) In addition to the binary sequences of period $N \equiv 0 \pmod 4$ constructed in [16] and [17], construct other families of binary sequences of period $N \equiv 0 (\bmod 4)$.

Acknowledgment

The authors wish to thank the referee for helpful comments and suggestions that improved the presentation of this correspondence.

References

[1] A. Chang, S. W. Golomb, G. Gong, and P. V. Kumar, "On ideal autocorrelation sequences arising from hyperovals," in *Sequences and Their Applications: Proc. SETA '98*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer-Verlag, 1999, pp. 17–38.

[2] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. New York: Wiley, 1989.

[3] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam, The Netherlands: North-Holland/Elsevier, 1998, North-Holland Mathematical Library 55.

[4] J. A. Davis, "Almost difference sets and reversible difference sets," *Arch. Math.*, vol. 59, pp. 595–602, 1992.

[5] L. E. Dickson, "Cyclotomy, higher congruences, and Waring's problem," *Amer. J. Math.*, vol. 57, pp. 391—424–463—474, 1935.

[6] C. Ding, "Binary cyclotomic generators," in *Fast Software Encryption (Lecture Notes in Computer Science)*, B. Preneel, Ed. New York: Springer-Verlag, 1995, vol. 1008, pp. 29–60.

[7] ——, "Cryptographic counter generators," Turku Center for Computer Science, TUCS Series in Dissertation 4, ISBN 4951-650-929-0, 1997.

[8] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2601–2606, Nov. 1999.

[9] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1996.

[10] H. Dobbertin, "Kasami power functions, permutation polynomials and cyclic difference sets," in *Proc. NATO ASI Workshop*, Aug. 3–14, 1998.

[11] S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA: Aegean Park, 1982.

[12] ——, "Cyclic Hadamard difference sets — Constructions and applications," in *Sequences and Their Applications: Proc. SETA '98*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer Verlag, 1999, pp. 39–48.

[13] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, Pless and Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. II, pp. 1765–1854.

[14] D. Jungnickel and A. Pott, "Difference sets: Abelian," in *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL: CRC, 1996, pp. 297–307.

[15] J.-H. Kim and H.-Y. Song, "Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," *J. Commun. and Networks*, vol. 1, no. 1, pp. 14–18, 1999.

[16] A. Lempel, M. Cohn, and W. L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 38–42, Jan. 1977.

[17] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee, and T. Helleseth, "New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$," paper, submitted for publication.

[18] J. -S. No, H. Chung, and M. -S. Yun, "Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1278–1282, May 1998.

[19] J.-S. No, S. W. Golomb, G. Gong, H.-K. Lee, and P. Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 44, pp. 814–817, Mar. 1998.

[20] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*. Rockville, MD: Computer Sci., 1985, vol. 1.

[21] ——, *Spread Spectrum Communications*, revised ed. New York: McGraw–Hill, 1994.

On Codes that Avoid Specified Differences

Bruce E. Moision, *Member, IEEE*,
Alon Orlitsky, *Senior Member, IEEE*, and Paul H. Siegel, *Fellow, IEEE*

***Abstract*—Certain magnetic recording applications call for a large number of sequences whose differences do not include certain disallowed binary patterns. We show that the number of such sequences increases exponentially with their length and that the growth rate, or capacity, is the logarithm of the joint spectral radius of an appropriately defined set of matrices. We derive a new algorithm for determining the joint spectral radius of sets of nonnegative matrices and combine it with existing algorithms to determine the capacity of several sets of disallowed differences that arise in practice.**

***Index Terms*—Capacity, constrained coding, joint spectral radius, magnetic recording.**

I. Introduction

The error probability of many magnetic-recording systems may be characterized in terms of the differences between the sequences that may be recorded [1]–[3]. In fact, the bit-error rate (BER) is often dominated by a small set of potential difference patterns. Recently, binary codes have been proposed which exploit this fact [4]–[9]. The codes are designed to avoid the most problematic difference patterns by constraining the set of allowed recorded sequences and have been shown to improve system performance.

In this correspondence, we study the largest number of sequences whose differences exclude a given set of disallowed patterns. We show that the number of such sequences increases exponentially with their length and that the growth rate, or capacity, is the logarithm of the joint spectral radius of an appropriately defined set of matrices. We derive new algorithms for determining the joint spectral radius of sets of nonnegative matrices and combine them with existing algorithms to determine the capacity of several sets of disallowed differences that arise in practice.

The correspondence is organized as follows. In the next section, we motivate the problem by summarizing known results showing that the error probability in models of magnetic recording systems is determined by the differences between recorded sequences. In Section III, we formally describe the resulting combinatorial problem, introduce the notation used, and present some simple examples. Section IV contains the main result of the correspondence, deriving the connection to

Manuscript received October 4, 1999; revised August 17. 2000. This work was supported by UC Micro Project 98-140 in cooperation with Marvell Semiconductor Incorporated, the Center for Magnetic Recording Research (UCSD), and under NSF Grant NCR-9612802. The material in this correspondence was presented in part at the 1999 IEEE Global Communications Conference (GLOBECOM'99), Rio de Janeiro, Brazil, December 5–9, 1999 and at the 2000 IEEE International Symposium on Information Theory (ISIT'00), Sorrento, Italy, June 25–30, 2000.

B. E. Moision was with the Mathematical Sciences Research Center, Lucent Technologies, Murray Hill, NJ 07974 USA. He is now with the Communications Systems and Research Section, Jet Propulsion Laboratory, Pasadena, CA 91101-8099 USA (e-mail: bmoision@shannon.jpl.nasa.gov).

A. Orlitsky and P. H. Siegel are with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093-0407 USA (e-mail: alon@ece.ucsd.edu: psiegel@ucsd.edu).

Communicated by R. M. Roth, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(01)00374-1.